



Medien Zeghid, PhD

Assistant Professor

m.zeghid@psau.edu.sa ; medien.zeghid@fsm.rnu.tn

Mobile: (+966)593624406 (KSA); (+216)55644603 (TUN);

Address

Electrical Engineering Department, College of Engineering,
Prince Sattam Bin Abdulaziz University P.O.Box: 54, Wadi
Addwasir (11991), Kingdom of Saudi Arabia.

MARITAL STATUS

Married.

DATE OF BIRTH

August 1, 1979

CAREER OBJECTIVES

Corresponding on scientific theoretical and practical background, I have gotten an experience in dealing with different facts and theorems. Depending on my ambition and activity, I am insisting to satisfy my goals in the short and long future:

- ✚ Keeping up with the cutting edge of technologies.
- ✚ Using my skills in the best possible way for achieving my professional goals.
- ✚ Seeking a responsible job with an opportunity for professional challenges.

ACADEMIC QUALIFICATIONS

- ✚ **Ph.D., Sciences and Technologies of Information and Communication**, University of South Brittany (Lorient-France). October 2011.
- ✚ **M.Sc., Microelectronic: Security of communication and information**, Faculty of Sciences of Monastir, Tunisia, July 2005. Grade (Excellent).
- ✚ **B.Sc., Microelectronic**: Faculty of Sciences of Monastir, Tunisia, June 2003. Grade (Good).
- ✚ **Habilitation for research and teaching**, Prepared at the laboratory of Electronic and Microelectronic of Faculty of Sciences of Monastir. Tunisia. This degree is under preparation, it will be presented soon (planned for November 2017).

ABILITIES/QUALITIES

- ✚ A strategic and creative thinker
- ✚ Ability to work either independently or collectively

- ✚ Demonstrated problem-solving and decision making ability

RESEARCH INTEREST

Cryptography, Architectural Synthesis for the Crypto-systems, System Modeling, Synthesis of communications for the SOC, Image & Video Coding, Adequacy Algorithm Architecture, High-level synthesis.

Academic Experience

- Sep. 2006 – Oct. 2011** Teaching & Research Assistant, Higher Institute of Applied Sciences and Technology, university of Sousse, Tunisia.
- Sep.2012 – June 2014** Assistant professor, Higher Institute of Applied Sciences and Technology University of Sousse, Tunisia.
- From Sep.2014** Assistant professor, Prince Sattam Bin Abdulaziz University, College of Engineering, Department of Electrical Engineering, Wadi Addwasir- Kingdom of Saudi Arabia.

TAUGHT COURSES

✚ Undergraduate (B.Sc.)

Computer Architecture ,Computer Organization & Assembly ,Microprocessor and Microcontroller , Embedded Computing, Real-Time Computing ,Digital communication, signal and systems analysis, Digital Signal Processing, Electrical and electronic engineering, Logic design.

✚ Graduate (M.Sc.)

Security in Embedded Systems

ACTIVITIES

1. Coordinator for Quality Assurance & Accreditation Unit, College of Engineering at Wadi Aldawaser, Prince Sattam Bin Abdulaziz University, KSA.
2. Member of the scientific committee in the Laboratory of Information Science and Technology, Communication and Knowledge, University of South Brittany (Lorient-France). Lab-STICC, UMR CNRS 6285, <http://www.lab-sticc.fr/>.
3. Member of the scientific committee in the Microelectronic Laboratory (Sciences Faculty of Monastir). <http://leme.tn/>.
4. Member in the scientific council at the laboratory of Electronic and Microelectronics at Monastir. –(2009-2012).
5. Member of the pedagogic committee of the technology department in the higher institute of Applied sciences and Technology of Sousse.
6. Member in the national (Tunisia) expert committee in Electronic and Microelectronics.
7. 2014 till now Reviewer with Journal of Circuits, Systems, and Computers.
8. 2014 till now Reviewer with International Journal of Open Information Technologies.

FUNDED RESEARCH PROJECTS

● September 2006 – June 2010

Name of the Project: (CMCU) MIC@R: (Tunisian French Joint Committee for University Cooperation) Modeling and Integration of virtual components IPs on architectures based on networks on chip NOC.

Responsible: Rached Tourki, Adel Baganne

Establishment: Laboratory of Information Science and Technology, Communication and Knowledge, University of South Brittany (Lorient-France) and Physical – Electronic and Microelectronic Laboratory (Sciences Faculty of Monastir, Tunisia).

● September 2008 – June 2011

Name of the Project: (CMCU) Study of the quality of service in the crypto-processors architectures.

Responsible: Rached tourki, Habib MEHREZ, Roselyne CHOTIN-AVOT

Establishment: Computing Laboratory of Paris 6, University Pierre & Marie Curie (Paris-France) and Physical – Electronic and Microelectronic Laboratory (Sciences Faculty of Monastir, Tunisia).

● September 2012

Laboratory of Electronic Antenna and telecommunication (LEAT) - Nice-Sophia Antipolis, France: Assistant Professor Alain Pegatoquet.

● September 2013: Present

Laboratory of Information Science and Technology, Communication and Knowledge, University of South Brittany (Lorient-France): Prof. Adel Baganne, Pof Guy Gogniat.

PUBLICATIONS : 1-Conference

1. Sonia Kotel, Fatma Sbiaa, *Medien Zeghid*, Mohsen Machhout, Adel Baganne, Rached Tourki, "Performance Evaluation and Design Considerations of Lightweight Block Cipher for Low-Cost Embedded Devices", 13th ACS/IEEE International Conference on Computer Systems and Applications AICCSA 2016 November 29th to December 2nd, 2016.
2. Sonia Kotel, Fatma Sbiaa, *Medien Zeghid*, Mohsen Machhout, Adel Baganne, Rached Tourki, "Efficient Hybrid Encryption System Based on Block Cipher and Chaos Generator", 16th IEEE International Conference on Computer and Information Technology Shangri-La's Fijian Resort and Spa, Fiji, 7-10 December 2016.
3. Fatma Sbiaa, Sonia Kotel, , *Medien Zeghid*, Mohsen Machhout, Adel Baganne, Rached Tourki, " A Selective Encryption Scheme with Multiple security Levels for the H.264/AVC Video Coding Standard", 16th IEEE International Conference on Computer and Information Technology Shangri-La's Fijian Resort and Spa, Fiji, 7-10 December 2016.
4. Fatma sbiaa, *Medien Zeghid*, Adel Baganne, Rached tourki, "Evaluation and a Chaos-Based improvement of a Block Cipher Algorithm",3rd International Conference on Automation, Control Engineering and Computer Science (ACECS-2016), 30 march 2016.
5. Anissa Sghaier, Chiraz Massoud, *Medien Zeghid* and Mohssen Machhoutm "Software Implementation of ECC Using GMP Library",3rd International Conference on Automation, Control Engineering and Computer Science (ACECS-2016), 30 march 2016.
6. Chiraz Massoud, Anissa Sghaier, *Medien Zeghid* and Mohssen Machhout, "EFFICIENT HARDWARE MULTIPLIER DESIGN FOR PAIRING COMPUTATION",16th international conference on Sciences and Techniques of Automatic control & computer engineering - STA'2015, Monastir, Tunisia, December 21-23, 2015.

7. Fatma sbiaa, *Medien Zeghid*, Adel Baganne “A new approach for encryption system based on block cipher algorithms and logistic function “,12th International Multi-Conference on Systems, Signals & Devices (SSD), March 2015.
8. Anissa Sghaier, *Medien Zeghid*, Mohssen Machhoutm "Proposed efficient arithmetic operations architectures for Hyperelliptic Curves Cryptosystems (HECC)", 12th International Multi-Conference on Systems, Signals & Devices (SSD), March 2015.
9. Fatma sbiaa, *Medien Zeghid*, Adel Baganne, Rached tourkim "An efficient Encryption scheme based on Block Cipher Algorithm"m 13th international conference on Telecommunications and informatics, December 2014. ISBN: 978-1-61804-262- 0, pp.133-138.
10. Sonia Kotel, *Medien Zeghid*, Adel Baganne, Rached tourki, "FPGA-Based Real-Time Implementation of AES Algorithm for Video Encryption", 13th international conference on Telecommunications and informatics, December 2014. ISBN: 978-1-61804-262-0, pp.27-36.
11. Yahia SALAH, *Medien Zeghid* and Rached TOURKI, " Conception et Intégration d’un IP de Sécurité pour les Architectures de Communication dans un SoC", The 2012 Sciences of Electronics, Technologies of Information and Telecommunications, Sousse Tunisia, 21-24 March 2012.
12. Yahia SALAH, *Medien Zeghid*, Imed E.BENNOUR and Rached TOURKI, " A Scheduling Approach for Packet-Switched on-Chip Networks", 2011 International Conference on Communications, Computing and Control Applications (CCCA 2011), Hammamet, Tunisia 3-5 March 2011. ISBN 978-1-4244-9795-9, pp.1-8.
13. Dhaha Dia, *Medien Zeghid*, Taoufik Saidani, Mohamed Atri, Belgacem Bouallegue, Mohsen Machhout and Rached Tourki, "Multi-level Discrete Wavelet Transform Architecture Design ", The 2009 International Conference of Computer Science and Engineering, London, U.K., 1-3 July, 2009. ISBN: 978-988-17012-5-1.
14. El hadj youssef, wajih; *Medien Zeghid*, Machhout, Mohsen; Bouallegue, Belgacem; Tourki, Rached, "Efficient hardware architecture of recursive Karatsuba-Ofman multiplier", 3rd International Conference on Design and Technology of Integrated Systems in Nanoscale Era, 2008. DTIS 2008. ISBN 978-1-4244-1576-2, pp.1-6.
15. *Medien Zeghid*, Bouallegue Belgacem, Baganne Adel, Machhout Mohsen and Tourki Rached, "Reconfigurable Implementation of the New Secure Hash Algorithm", The International Conference on Availability, Reliability and Security 2007 (ARES 2007), Vienna, April 10th-13th, 2007. ISBN- 0-7695-2775-2, pp.281-285.
16. *Medien Zeghid*, Mohsen Machhout, Lazhar Khriji, Adel Baganne and Rached Tourki, "A Modified AES Based Algorithm for Image Encryption", International Conference on Computer, Information and Systems Science and Engineering, Vienna, Austria May 25-27, 2007.

PUBLICATIONS : 2- Scientific journals

1. Fatma sbiaa, *Medien Zeghid*, Adel Baganne, Rached tourki “High-Level Implementation of a Chaotic and AES Based Crypto-system” *Accepted* paper to *appear* in Journal of Circuits, Systems, and Computers, Future Issue, 2017.
2. Hassan Yousif Ahmed, *Medien Zeghid*, K. S. Nisar S. A. Aljunid, “Numerical Method for Constructing Fixed Right Shift (FRS) Code for SAC-OCDMA Systems” in International Journal of Advanced Computer Science and Applications, V.8(1), pp.245-252,2017.
3. Anissa Sghaier, *Medien Zeghid*, Loubna Ghammam, Sylvain Duquesne, Mohsen Machhout, “Area-Efficient Hardware Implementation of the Optimal Ate Pairing over BNCurves” submitted in Microprocessors and Microsystems Journal, February 2017.
4. Fatma sbiaa, *Medien Zeghid*, Adel Baganne, Mohssen Machhout, Rached tourki “A chaos based approach for correcting the security level of a block cipher algorithm” in International Review on Computers and Software, V.11(2), 2016.
5. Fatma sbiaa, *Medien Zeghid*, Sonia Kotel, Adel Baganne, Mohssen Machhout, Rached tourki “A Format-Compliant Selective Encryption Scheme for Real-Time Video Streaming of the H.264/AVC” in International Journal of Advanced Computer Science and Applications, V.7(4), pp.386-396,2016.

6. Anissa Sghaier, **Medien Zeghid** and Mohsen Machhout. Article, "Differential Fault Attacks and Countermeasures in Elliptic Curve Cryptography" in International Journal of Computer Applications V. 140(6), pp.1-6, April 2016.
7. Anissa Sghaier, Chiraz Massoud, **Medien Zeghid** and Mohsen Machhout, "Flexible Hardware Implementation of Hyperelliptic Curves Cryptosystem " in International Journal of Computer Science and Information Security, V.14(4),pp.1-7,2016.
8. **Medien Zeghid**, Anissa Sghaier, Chiraz Massoud, Mohsen Machhout, "Design And Implementation of Low Area/Power Elliptic Curve Digital Signature Hardware Core", submitted to Advances in Electrical and Computer Engineering- Journal, December 2016.
9. **Medien Zeghid**, Fatma sbiaa, Adel Baganne, Guy Gogniat, MOHSEN, " An Efficient selective Multiple security Levels scheme for the H.264 Video Coding" Submitted in Journal of Real-Time Image Processing, 2016.
10. Anissa Sghaier, **Medien Zeghid**, Belgacem Bouallegue, Adel Baganne, Mohsen Machhout "Area-Time Efficient Hardware Implementation of Elliptic Curve Cryptosystem" submitted in Journal of Circuits, Systems, and Computers, December 2016.
11. **Medien Zeghid**, Machhout MOHSEN, Belgacem Bouallegue, Lazhar Khriji, Adel Baganne and Tourki RACHED, "Design and Hardware Implementation of QoS-AES Processor for Multimedia applications" in Transactions on Data Privacy Journal, V.3(1), pp.43 – 64, 2010.
12. Mohsen Machhout, **Medien Zeghid**, El hadj Youssef Wajih, Belgacem Bouallegue and Rached Tourki, " Efficient Large Numbers Karatsuba-Ofman Multiplier Designs for Embedded Systems " in International Journal of Electronics, Circuits and Systems, V.3(1), pp.1 – 10, 2009.
13. Machhout Mohsen, Guitouni ZIED, **Medien Zeghid** and Tourki Rached, "Design of Reconfigurable Image Encryption Processor using 2-D Cellular Automata Generator" in International Journal of Computer Science and Applications, V.6(4), pp. 43 – 62, 2009.
14. **Medien Zeghid**, Belgacem Bouallegue, Mohsen Machhout, Adel Baganne and Rached Tourki, "Architectural design features of a programmable high throughput reconfigurable SHA-2 Processor", in Journal of Information Assurance and Security, V.3(2), pp.147 – 158, 2008.
15. Guitouni ZIED, Machhout Mohsen, **Medien Zeghid** and Tourki Rached, "A Comparison of Architecture Design and FPGA Implementation of Programmable Cellular Automata Generator and Stream Generators" in International Journal of Computer Sciences and Engineering Systems, V.2(3), pp.185– 192, 2008.
16. **Medien Zeghid**, Mohsen Machhout, Lazhar Khriji, Adel Baganne and Rached Tourki, "A Modified AES Based Algorithm for Image Encryption", in International Journal of Computer Science and Engineering, V.1(1), pp.70 – 75, 2007.
17. El hadj Youssef Wajih, **Medien Zeghid**, Mohsen Machhout, Belgacem Bouallegue and Rached Tourki, "Design and Performance testing of Arithmetic Operators Library for Cryptographic applications" in International Journal of Computer Sciences and Engineering Systems, V.1(3), pp.201 – 212, 2007.

Supervising Graduate Students

During my research activity I have proposed and advised several Post-graduate students

- ✓ **Master thesis:** Master of Communication and intelligent systems at the National School of Engineer of Sousse, Tunisia.
 - ✓ Name of candid: *Sbiaa Fatma (M.Sc., 2012)*
 - ✓ Name of candid: *Sonia Kotel (M.Sc., 2013)*
 - ✓ Name of candid: *Fadia Bouhleb (M.Sc., 2013)*
 - ✓ Name of candid: *Chiraz Massoud (M.Sc., 2016)*
- ✓ **PhD thesis: Phd, Sciences and Technologies of Information and Communication**
 - ✓ Name of candid: *Sbiaa Fatma (Phd, 2016)*
 - ✓ Name of candid: *Anissa Sghaier (Phd, 2016)*
 - ✓ Name of candid: *Sonia Kotel (Phd, in progress)*

✓ Name of candid: *Hammadi Mohsen (Phd, in progress)*

Laboratory of Information Science and Technology, Communication and Knowledge (Lab-STICC) in collaboration with the Microelectronic Laboratory (LEME), Sciences Faculty of Monastir, Tunisia.

COMPUTER PROFICIENCY

Experience in computer systems: modeling, programming and simulation, maintenance, repair, and operations, software for technical writing and drawing graphs and in software for teaching Electronic and physics.

COMPUTER KNOWLEDGE

✓ **Programming languages**

Mastering programming languages: Turbo Pascal, Turbo C, Visual C++, Matlab, Maple, Assembly.

Mastering the programming language: SystemC & VHDL.

✓ **Softwares**

Operating systems: Dos, Unix et MS-Windows.

Tables: Excel, Quattro-Pro

Design: Proteus ISIS, Power-Point and Correl-Draw.

Treatment: Word, Write, Word-Pad and Lotus-Organizer.

Conception tools: Synopsys, Encounter, Xilinx ISE and QUARTUS.